数理解析研究所講究録 第2120巻 2019年 52-61

THE p-ADIC UNIFORMISATION OF MODULAR CURVES BY p-ARITHMETIC GROUPS

HENRI DARMON

Abstract. This is a transcription of the author's lecture at the Kyoto conference "Profinite monodromy, Galois representations, and complex functions" marking Yasutaka Ihara's 80th birthday. Much of it, notably the material in the last section, is the fruit of an ongoing collaboration with Jan Vonk.

In his important work on "congruence monodromy problems", Professor Ihara proposed that the group $\Gamma := \mathbf{SL}_2(\mathbb{Z}[1/p])$ acting on the product of a Drinfeld and a Poincaré upper half-plane provides a congenial framework for describing the ordinary locus of the j-line in characteristic p. In Ihara's picture, which rests on Deuring's theory of the canonical lift, the ordinary points of the j-line are essentially in bijection with conjugacy classes in Γ that are hyperbolic at p and elliptic at ∞.

The present note explains how the classes that are elliptic at p and hyperbolic at ∞ form the natural domain for a kind of p-adic uniformisation of the modular curve $X_0(p)$, leading to a conjectural analogues of Heegner points, elliptic units, and singular moduli defined over ring class fields of real quadratic fields.

Contents

Introduction

My first encounter with Professor Ihara dates back to the 1990 International Congress of Mathematicians which took place right here in Kyoto when I was still a graduate student. My most vivid memory from that congress was Ihara's plenary lecture entitled "Braids, Galois groups, and some arithmetic functions". Its theme was the study of the absolute Galois group of $\mathbb{Q}$ through its natural action on the étale fundamental groups of curves and varieties. The subject was then in its early stages but has been very active in the ensuing decades, notably in Japan. At the time, I was keenly interested in this topic, having just finished taking the notes for a course given by Jean-Pierre Serre at Harvard, which eventually led to the monograph "Topics in Galois theory". One of the highlights of Serre's course was his exposition of the celebrated "rigidity method" of Malle and Matzat for realising certain finite groups as Galois groups of $\mathbb{Q}$ by exhibiting them as Galois groups of étale covers of $\mathbb{P}_1 - \{0, 1, \infty\}$. With Serre's course fresh in my mind, Ihara's plenary lecture made a tremendous impression on me.

This was the first but certainly not the last time that I would derive inspiration from Professor Ihara. The present note describes how his fundamental treatise [Ih] on "congruence monodromy problems" motivates an approach to the p-adic uniformisation of modular curves via the second cohomology of p-arithmetic groups, opening a natural pathway to explicit class field theory for real quadratic fields.

In [Ih], Ihara proposed that congruence subgroups $\Gamma \subset \mathbf{SL}_2(\mathbb{Z}[1/p])$ lead to a convenient framework for the "uniformisation" of modular curves in characteristic p. In a suggestive re-interpretation of classical results of Deuring on the canonical lift, Ihara observed that the conjugacy classes of Γ which are hyperbolic at p and elliptic at ∞ are essentially in bijection with the ordinary points on the characteristic p fiber of a modular curve attached to Γ. The natural desire to reverse the roles of p and ∞ in Ihara's theory leads one to consider the conjugacy classes of Γ that are hyperbolic at ∞ and elliptic at p, whose characteristic polynomials split over real quadratic fields in which the prime p is inert or ramified. Roughly speaking, suitable "canonical lifts" attached to such classes yield invariants that are defined over ring class fields of real quadratic fields. I will flesh out this statement by describing how groups like Γ provide an amenable structure for the p-adic uniformisation of modular curves, and how this uniformisation is rich enough to support a framework for "explicit class field theory" and a theory of singular moduli for real quadratic fields.

1. The p-adic uniformisation of Shimura curves

As background and motivation, let us briefly recall some facts from the theory of p-adic uniformisation of curves developped by Tate and Mumford. For this purpose, let Γ be a *discrete arithmetic subgroup* of $\mathbf{SL}_2(\mathbb{Q}_p)$. A protoypical example of such a group is obtained by letting

$$\mathbb{H} := \mathbb{Q}[i, j, k]$$

be the algebra of Hamilton quaternions over the field $\mathbb{Q}$ of rational numbers, defined by the usual multiplication rules

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

If p is an odd prime, then

$$\mathbb{H} \otimes \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p),$$

and one can therefore fix an algebra embedding of $\mathbb{H}$ into the matrix algebra $M_2(\mathbb{Q}_p)$. The subring

$$R := \mathbb{Z}[i, j, (1 + i + j + k)/2]$$

studied by Hurwitz is a maximal order in $\mathbb{H}$, and is unique up to conjugation by $\mathbb{H}^\times$. The group

$$\Gamma := R[1/p]_1^\times \subset \mathbf{SL}_2(\mathbb{Q}_p)$$

of norm 1 elements in the associated maximal $\mathbb{Z}[1/p]$-order acts discretely by Möbius transformations on Drinfeld's p-adic upper half plane

$$\mathcal{H}_p := \mathbb{C}_p - \mathbb{Q}_p.$$

The quotient $\Gamma\backslash\mathcal{H}_p$ is a rigid analytic space, which is isomorphic to the $\mathbb{C}_p$-points of a "Mumford curve" X_Γ over $\mathbb{Q}_p$.

The following theorem, a special case of the Cerednik-Drinfeld theorem on the p-adic uniformisation of Shimura curves, gives a modular description of X_Γ, which shows in particular that it has a model over $\mathbb{Q}$.

Theorem 1 (Cerednik-Drinfeld). *The curve X_Γ is isomorphic to a Shimura curve (classifying abelian surfaces with quaternionic multiplication by the quaternion algebra ramified at 2 and p).*

One would be remiss not to mention that Ihara's work on "congruence monodromy problems" plays a key role in the proof of this important result of Cerednik-Drinfeld.

Shimura curves are endowed with a plethora of interesting arithmetic structure, notably an infinite supply of CM points attached to orders of quadratic imaginary fields in which the prime p is either inert or ramified.

Let $K \subset \mathbb{H}$ be any maximal commutative subfield of $\mathbb{H}$. It is isomorphic to a quadratic imaginary field (in which 2 is either inert or ramified), and $K \cap R[1/p]$ is a (not necessarily maximal) $\mathbb{Z}[1/p]$-order in K – i.e., a subring of K which is free of rank two as a $\mathbb{Z}[1/p]$-module. Such an order is completely characterised by its conductor, an integer c that is prime to p and satisfies

$$K \cap R[1/p] = \mathbb{Z}[1/p] + c \cdot \mathcal{O}_K[1/p].$$

The theory of complex multiplication for the Shimura curve X_Γ can be formulated concretely as follows:

Proposition 2. *Suppose that the prime p is either inert or ramified in K, so that $K^\times$ acting on $\mathcal{H}_p$ has two fixed points in $\mathcal{H}_p$. Then these fixed points correspond to* algebraic *points of X_Γ, defined over the ring class field of K of conductor c.*

Turning to the function theory of X_Γ, let $\mathcal{M}^\times$ denote the multiplicative group of rigid meromorphic functions on $\mathcal{H}_p$, and let $\mathcal{A}^\times$ denote the subgroup of rigid analytic functions. Constructing non-zero meromorphic functions on $X_\Gamma(\mathbb{C}_p)$ is tantamount to constructing Γ-invariant elements of $\mathcal{M}^\times$, i.e., elements of $H^0(\Gamma, \mathcal{M}^\times)$.

The standard way to do this is via the theory of p-adic theta functions, as described for instance in the monograph [GvdP] of Gerritzen and van der Put.

Given any divisor $\Delta \in \mathrm{Div}^0(\mathcal{H}_p)$, and a base point $\eta \in \mathcal{H}_p$, let

$$t^\eta_\Delta(z) := \text{ unique function with divisor } \Delta \text{ with } t^\eta_\Delta(\eta) = 1.$$

The p-adic theta-function atttached to Δ is then defined by averaging t^η_Δ over the Γ-translates of Δ:

$$\theta_\Delta(z) := \prod_{\gamma \in \Gamma} t^\eta_{\gamma(\Delta)}(z).$$

Since θ_Δ has a Γ-invariant divisor, it belongs to $H^0(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times)$, i.e.,

$$\theta_\Delta(\gamma z) = c_\Delta(\gamma) \cdot \theta_\Delta(z), \qquad \text{for all } \gamma \in \Gamma.$$

The *automorphy factor* $c_\Delta : \Gamma \longrightarrow \mathbb{C}_p^\times$ is a homomorphism, i.e., an element of $H^1(\Gamma, \mathbb{C}_p^\times)$, which measures the obstruction to θ^η_Δ being Γ-invariant, and thereby, to the divisor Δ being principal on X_Γ.

The group $\Pi_\Gamma \subset H^1(\Gamma, \mathbb{C}_p^\times)$ generated by the automorphy factors of elements of $H^0(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times)$ plays an important role in describing the Jacobian of X_Γ over $\mathbb{C}_p$. It is a *lattice* in $H^1(\Gamma, \mathbb{C}_p^\times) \simeq (\mathbb{C}_p^\times)^g$, and there is a rigid analytic, Hecke-equivariant map

$$\eta : H^1(\Gamma, \mathbb{C}_p^\times)/\Pi_\Gamma \longrightarrow \mathrm{Jac}(X_\Gamma)(\mathbb{C}_p),$$

which fits into the following commutative diagram:

(1)
$$\begin{array}{ccccccc}
 & & & & H^0(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times) & \xrightarrow{\delta} & \Pi_\Gamma \\
 & & & & \downarrow & & \downarrow \\
\mathbb{C}_p^\times & \hookrightarrow & H^0(\Gamma, \mathcal{M}^\times) & \longrightarrow & H^0(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times) & \xrightarrow{\delta} & H^1(\Gamma, \mathbb{C}_p^\times) \\
 & & \downarrow \mathrm{Div} & & \downarrow \mathrm{Div} & & \downarrow \eta \\
 & & P(X_\Gamma) & \hookrightarrow & \mathrm{Div}^0(X_\Gamma) & \xrightarrow{\Phi} & \mathrm{Jac}(X_\Gamma)(\mathbb{C}_p).
\end{array}$$

Thus, for instance, the automorphy factor attached to the theta function of a CM divisor Δ is sent by η to an element of $\mathrm{Jac}(X_\Gamma)(\mathbb{C}_p)$ which is algebraic, and defined over a ring class field of an imaginary quadratic field. This concrete description leads to a rigid analytic approach for numerically computing Heegner points arising from parametrisations of elliptic curves by Shimura curves. (See [Gr].)

2. The p-adic uniformisation of $X_0(p)$

We now turn to the setting of classical modular curves, which, unlike Shimura curves, do not seem to admit uniformisations via *explicit* arithmetic subgroups of $\mathbf{SL}_2(\mathbb{Q}_p)$. For example, the modular curve $X_0(p)$ is a Mumford curve — it has an integral model whose special fiber is a union of two copies of the j-line intersecting transversally at the supersingular points — hence Mumford's p-adic uniformization theorem implies the existence of *some* discrete subgroup $\Gamma \subset \mathbf{SL}_2(\mathbb{Q}_p)$, for which

$$X_0(p)(\mathbb{C}_p) \simeq \Gamma\backslash\mathcal{H}_p.$$

To what extent can Γ be described explicitly? Is it arithmetic, for instance? Very little seems to be known.

In his celebrated monographs on "Congruence monodromy problems", Ihara proposed that the group

$$\Gamma = \mathbf{SL}_2(\mathbb{Z}[1/p])$$

in some sense "uniformises" the j-line in characteristic p. More precisely, the conjugacy classes in Γ that are hyperbolic at p and elliptic at ∞, corresponding to orders in quadratic imaginary fields where p is split, are essentially in bijection with ordinary points on $X(1)$ in characteristic p. This leads to an elegant, inspiring re-formulation of the results of Deuring on complex multiplication and of his theory of the canonical lift.

Guided by Ihara's vision, the same Γ can be used as the basis for a "p-adic uniformisation" of $X_0(p)$. In this theory, a key role is played by conjugacy classes in Γ that are hyperbolic at ∞ and elliptic at p, corresponding to orders in *real* quadratic fields where p is non-split.

The group Γ acts on $\mathcal{H}_p$ with *dense orbits* in the rigid topology, and hence

$$H^0(\Gamma, \mathcal{A}^\times) = H^0(\Gamma, \mathcal{M}^\times) = \mathbb{C}_p^\times.$$

The key insight in extending Cerednik-Drinfeld theory to the group Γ is to replace the (uninteresting) zero-th cohomology of Γ with values in $\mathcal{A}^\times$ and $\mathcal{M}^\times$ with its *first cohomology*:

Definition 3 [DV1]**.** *A* rigid meromorphic cocycle *is a class in* $H^1(\Gamma, \mathcal{M}^\times)$ *which is* quasi-parabolic*: i.e., its restriction to* $\Gamma_\infty := \mathrm{Stab}_\Gamma(\infty)$ *belongs to* $H^1(\Gamma_\infty, \mathbb{C}_p^\times)$.

Definition 3 raises the question of constructing non-trivial elements of $H^1(\Gamma, \mathcal{M}^\times)$, and of classifying them. It turns out that rigid meromorphic cocycles are intimately tied with certain *quasi-periodic subsets* of the set of *real multiplication* (RM) points of $\mathcal{H}_p$:

Definition 4. *An RM point is an element of* $\mathcal{H}_p$ *which belongs to a real quadratic field* $K \subset \mathbb{C}_p$.

All the real quadratic fields which shall arise are viewed as subfields of $\mathbb{R}$ as well as of $\mathbb{C}_p$, and the symbol w' is used to denote the algebraic conjugate of a real quadratic irrationality w. For any w in the set $\mathcal{H}_p^{\mathrm{RM}}$ of RM points in $\mathcal{H}_p$, and $r \in \mathbb{Q}$, one can thus consider the sign function

$$s(w,r) := \begin{cases} 1 & \text{if } w' < r < w, \\ -1 & \text{if } w < r < w', \\ 0 & \text{otherwise} \end{cases}$$

Lemma 5. *The set* Π_τ *of* $w \in \Gamma\tau$ *with* $s(w,r) \neq 0$ *is a discrete subset of* $\mathcal{H}_p$.

The subset of $\Gamma\tau$ described in this lemma is somewhat reminiscent of the "almost periodic" structures arising in the theory of quasi-crystals.

Lemma 5 makes it possible to define certain *quasi-periodic theta functions* whose zeroes and poles are concentrated in Π_τ:

Proposition 6. *The infinite product*

$$\theta_\tau[r](z) := \prod_{w \in \Gamma\tau} t_{w-\infty}^{\eta}(z)^{s(w,r)}$$

converges to a rigid meromorphic function on $\mathcal{H}_p$.

The function $\theta_\tau[r](z)$ is called the *quasi-periodic theta function* associated to τ and r. Its divisor is supported on a small (discrete) subset of the full Γ-orbit of τ in $\mathcal{H}_p$. The collection of $\theta_\tau[r]$ as r varies over $\mathbb{P}_1(\mathbb{Q})$ can be packaged into a single *rigid meromorphic cocycle modulo scalars*, according to the following definition:

Theorem 7 [DV1]**.** *The function* $J_\tau : \Gamma \longrightarrow \mathcal{M}^\times$ *given by*

$$J_\tau(\gamma) = \theta_\tau[\gamma\infty]$$

is a one-cocycle with values in $\mathcal{M}^\times/\mathbb{C}_p^\times$. *All elements of* $H^1(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times)$ *are multiplicative combinations of the* J_τ *as* τ *ranges over* $\mathcal{H}_p^{\mathrm{RM}}$, *and of elements of* $H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times)$.

The theory of rigid meromorphic cocycles seems intimately tied to the arithmetic of real quadratic fields via this result.

The cocycles

$$J_\tau \in H^1(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times)$$

are called *theta-cocycles*. They are the direct analogues of the p-adic theta functions in $H^0(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times)$ when Γ is a p-adic Schottky group. The analogue of the automorphy factor associated to such a p-adic theta function is the invariant

$$\delta(J_\tau) \in H^2(\Gamma, \mathbb{C}_p^\times)$$

arising from the long exact cohomology sequence

$$H^1(\Gamma, \mathbb{C}_p^\times) \longrightarrow H^1(\Gamma, \mathcal{M}^\times) \longrightarrow H^1(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times) \xrightarrow{\delta} H^2(\Gamma, \mathbb{C}_p^\times),$$

which measures the obstruction to lifting J_τ to a genuine rigid meromorphic cocycle.

The following basic fact about $H^2(\Gamma, \mathbb{C}_p^\times)$, which was first systematically exploited in the work of Ihara and Serre, suggests that this p-adic torus might bear some connection to the uniformisation of $X_0(p)$:

Proposition 8 (Ihara, Serre). *There is a canonical identification*

$$H^2(\Gamma, \mathbb{C}_p^\times) = H^1(\Gamma_0(p), \mathbb{C}_p^\times)$$

of p-adic tori which is compatible with the natural action of Hecke operators on source and target.

The theory of theta-cocycles thus associates to each divisor Δ on $\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}}$ a cocycle

$$J_\Delta \in H^1(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times).$$

Definition 9. *If J_Δ lifts to a rigid meromorphic cocycle, then Δ is called a* principal divisor*.*

Denote by $P(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}})$ the group of principal divisors, and let $M_2(\Gamma_0(p))$ be the space of weight two modular forms on $\Gamma_0(p)$. The following theorem implies that principal divisors, and hence rigid meromorphic cocycles, exist in abundance:

Theorem 10 [DV1]**.** *If T is any Hecke operator that annihilates $M_2(\Gamma_0(p))$, and τ any element of $\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}}$ (or any divisor on this quotient), then $T(\tau)$ is principal.*

Corollary 11. *The quotient* $\mathrm{Div}(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}})/P(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}})$ *is naturally a module for the Hecke algebra of weight* 2 *and level* p*.*

Pursuing the analogy with the p-adic uniformisation of Mumford curves, the group

$$\Pi_\Gamma := \delta(H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times) \subset H^2(\Gamma, \mathbb{C}_p^\times)$$

should play the same role as the subgroup $\Pi_\Gamma \subset H^1(\Gamma, \mathbb{C}_p^\times)$ attached to the p-adic Shottky group Γ in equation (1). Indeed, one has:

Theorem 12 (Dasgupta, D). *The image of Π_Γ in*

$$H^2(\Gamma, \mathbb{C}_p^\times) = H^1(\Gamma_0(p), \mathbb{C}_p^\times)$$

is commensurable to the direct sum of $p^{\mathbb{Z}}$ with two copies of the Tate period lattice of $J_0(p)$.

The proof of this result, which is described in [Das], is far from formal and relies on several deep ingredients, notably the "exceptional zero" conjecture of Mazur, Tate and Teitelbaum, and its proof by Greenberg and Stevens [GS], which rests crucially on the theory of deformations of p-adic Galois representations.

The discussion so far can be summarised in the following analogue of the commutative diagram (1), in which the cohomology degrees have been shifted by one, and the rows and columns are exact up to finite kernels and cokernels:

(2)
$$\begin{array}{ccccc} & & H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times) & \xrightarrow{\delta} & \Pi_\Gamma \\ & & \downarrow & & \downarrow \\ H^1(\Gamma, \mathcal{M}^\times) & \longrightarrow & H^1(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times) & \xrightarrow{\delta} & H^2(\Gamma, \mathbb{C}_p^\times) \\ \downarrow \mathrm{Div} & & \downarrow \mathrm{Div} & & \downarrow \eta \\ P(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}}) & \hookrightarrow & \mathrm{Div}(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}}) & \xrightarrow{\Phi} & J_0(p)^2(\mathbb{C}_p) \oplus \mathbb{C}_p^\times/p^{\mathbb{Z}}. \end{array}$$

Now, given $\tau \in \mathcal{H}_p^{\mathrm{RM}}$, let

$$\mathcal{O}_\tau = \{\gamma \in M_2(\mathbb{Z}[1/p]) \text{ such that } \gamma\tau = \tau\} \subset K := \mathbb{Q}(\tau).$$

Class field theory associates to the order $\mathcal{O}_\tau$ a ring class field of K, denoted H_τ, with $\mathrm{Gal}(H_\tau/K) = \mathrm{Pic}(\mathcal{O}_\tau)$. One of the "main conjectures of real multiplication" can be stated as follows [Dar]:

Conjecture 13. *For all $\tau \in \mathcal{H}_p^{\mathrm{RM}}$, the point $\Phi(\tau)$ belongs to $J_0(p)^2(H_\tau) \oplus H_\tau^\times/p^{\mathbb{Z}}$ (up to torsion).*

This conjecture suggests that the uniformisation Φ carries a great deal of arithmetic structure, enabling the analytic construction of points on elliptic curves defined over ring class fields of real quadratic fields, thus holding out the prospect for a natural extension of the classical theory of complex multiplication.

3. Singular moduli for real quadratic fields

Of crucial importance to the notion of *singular moduli* in the theory of "real multiplication" is the fact that it is possible to evaluate a rigid meromorphic cocycle at an RM point. This rests on the simple fact that an element $\tau \in \mathcal{H}_p$ is an RM point if and only if

$$\mathrm{Stab}_\Gamma(\tau) = \langle \pm\gamma_\tau \rangle$$

is an infinite group of rank one. One is thus led to make the following definition:

Definition 14. *If $J \in H^1(\Gamma, \mathcal{M}^\times)$ is a rigid meromorphic cocycle, and $\tau \in \mathcal{H}_p$ is an RM point, then the* value *of J at τ is*

$$J[\tau] := J(\gamma_\tau)(\tau) \in \mathbb{C}_p \cup \{\infty\}.$$

The quantity $J[\tau]$ is a well-defined numerical invariant, independent of the cocycle representing the class of J, and

$$J[\gamma\tau] = J[\tau], \qquad \text{for all } \gamma \in \Gamma.$$

We now turn to describing the *field of definition* of a rigid meromorphic cocycle:

Definition 15. *If*

$$J = \prod_{i=1}^{n} J_{\tau_i}^{n_i}$$

is a rigid meromorphic cocycle, then

$$H_J := \text{Compositum}(H_{\tau_i})$$

is called the field of definition *of J.*

With these notions in hand, the "main conjectures" of "real multiplication" can be stated loosely as follows:

Conjecture 16 [DV1]**.** *Let J be a rigid meromorphic cocycle, and let $\tau \in \mathcal{H}_p$ be an RM point. The value $J[\tau]$ belongs to the compositum of H_J and H_τ.*

Conjecture 17 ("Shimura reciprocity"). *If $\tau_1, \ldots, \tau_h$ are representatives for the $h = \#Pic^+(\mathcal{O})$ distinct Γ-orbits of RM attached to $\mathcal{O}$, the values $\{J[\tau_j]\}_{1\le j\le h}$ are permuted by $\text{Gal}(H_J H_{\mathcal{O}}/H_J)$.*

In order to illustrate the above conjectures, we note that perhaps the simplest class of rigid meromorphic cocycles can be obtained via the following proposition:

Proposition 18 [DV1]**.** *For all $\tau \in \mathcal{H}_p^{\text{RM}}$, the divisor $(\tau) - (p\tau)$ is principal if $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$, (i.e., if p divides the cardinality of the Monster sporadic simple group, i.e., the curve $X_0(p)/w_p$ has genus zero.).*

For a prime p as above, let

$$J_\tau^+ := \text{ (unique) lift of} J_\tau/J_{p\tau} \text{ to } H^1(\Gamma, \mathcal{M}^\times).$$

For instance, assume that the prime p above satisfies the further condition $p \equiv 2, 3 \pmod 5$, i.e., that

$$p \in \{2, 37, 13, 17, 23, 47\},$$

and let

$$\omega := \frac{1+\sqrt{5}}{2} \quad \in \quad \mathcal{H}_p$$

be the golden ratio.

The cocycle J_ω^+ can in some sense be viewed as the "simplest" instance of a rigid meromorphic cocycle. Since $h^+(\mathbb{Q}(\sqrt{5})) = 1$, the field of definition of J_ω^+ is $\mathbb{Q}(\sqrt{5})$. Experiments suggest that J_ω^+ is in fact defined over $\mathbb{Q}$. Here are some empirical values of J_ω^+, obtained by calculating them numerically to at least 100 digits of p-adic accuracy and then recognising them as algebraic numbers of small height:

• If $\tau = 2\sqrt{2}$, then $H_\tau = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$, and

$$J_\omega^+[2\sqrt{2}] \stackrel{?}{=} (33 + 56\sqrt{-1})/(5 \cdot 13) \qquad (\text{in } \mathbb{C}_3)$$
$$J_\omega^+[2\sqrt{2}] \stackrel{?}{=} (1 + 2\sqrt{-2})/3 \qquad (\text{in } \mathbb{C}_{13}).$$

• If $\tau = 2\sqrt{6}$, then $H_\tau = \mathbb{Q}(\sqrt{6}, \sqrt{-1}, \sqrt{2})$, and

$$J_\omega^+[2\sqrt{6}] \stackrel{?}{=} (3 + 8\sqrt{2} + 12\sqrt{-1} + 2\sqrt{-2})/17 \qquad (\text{in } \mathbb{C}_7)$$
$$J_\omega^+[2\sqrt{6}] \stackrel{?}{=} (2 + 3\sqrt{2} + \sqrt{-3} + 2\sqrt{-6})/7 \qquad (\text{in } \mathbb{C}_{17}).$$

On the basis of the experiments above and of many more like them, we are led to make the following conjecture:

Conjecture 19 [DV1]**.** *The RM value $J_\omega^+[\tau]$ belongs to $H_\tau^{\sigma_p\sigma_\infty=1}$.*

Here is a further numerical example illustrating Conjecture 19, in the case where τ generates a real quadratic field $K := \mathbb{Q}(\sqrt{223})$ of narrow class number 6, whose narrow Hilbert class field H, a sextic extension of K, is therefore nonabelian over $\mathbb{Q}$. In line with Conjectures 17 and 18, the value $J_\omega^+[\sqrt{223}]$ seems to satisfy the polynomials:

$282525425x^6 + 27867770x^5 + 414793887x^4 - 128906260x^3 + 414793887x^2 + 27867770x + 282525425,$

$$464800x^6 + 1275520x^5 + 1614802x^4 + 1596283x^3 + 1614802x^2 + 1275520x + 464800,$$

and

$$4x^6 + 4x^5 + x^4 - 2x^3 + x^2 + 4x + 4,$$

for $p = 7, 13$ and 47 respectively.

Although the algebraicity of the RM values of rigid meromorphic cocycles remains elusive for now, good theoretical evidence is given in [DV2] for the algebraicity of the so-called *cuspidal values* of rigid meromorphic cocycles, which are defined as follows.

Definition 20. *If J is a rigid meromorphic cocycle, the quantity*

$$J\begin{pmatrix} p & * \\ 0 & 1/p \end{pmatrix} \in \mathbb{C}_p^\times$$

is called the value of *J at ∞ and denoted $J[\infty]$.*

Theorem 21 [DV2]**.** *For all J, the value $J[\infty]$ is algebraic. More precisely, a power of it belongs to $(\mathcal{O}_{H_J}[1/p])^\times$.*

The key ingredient in the proof of Theorem 21 is the fundamental recent progress towards the refinements of the p-adic Gross Stark conjectures formulated in [DD] that was made by Samit Dasgupta and Mahesh Kakde [DK], building on the methods of [DDP]. A key role is played in [DDP] and [DK] by the deformation theory of p-adic Galois representations, whose availability accounts for the fact that the p-adic Stark-conjectures are more tractable than their original archimedean counterparts.

It is worth insisting that rigid meromorphic cocycles do not arise from Hecke eigenforms, and their RM values have no direct relation to special values of L-functions with Euler products. The approach to explicit class field theory based on these RM values therefore represents something of a departure from the "traditional" framework of the Stark conjectures which rest on the leading terms of motivic L-functions.

One would like a better geometric understanding of the p-adic uniformisation theory described in this talk, dispensing with the seemingly ad-hoc techniques based on deformations of Galois representations, and tying it more closely with the fascinating perspectives opened up in Ihara's treatise on "Congruence monodromy problems".

References

[Dar] H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*. Ann. of Math. **154** (2001), 589–639.

[DD] H. Darmon and S. Dasgupta. *Elliptic units for real quadratic fields*. Ann. of Math. (2) **163** (2006), no. 1, 301–346.

[DDP] S. Dasgupta, H. Darmon, and R. Pollack, *Hilbert modular forms and the Gross-Stark conjecture*. Ann. of Math. (2) **174** (2011), no. 1, 439–484.

[DK] S. Dasgupta and M. Kakde, work in progress.

[DV1] H. Darmon and J. Vonk. *Singular moduli for real quadratic fields: a rigid analytic approach*. Submitted.

[DV2] H. Darmon and J. Vonk. *The cuspidal values of rigid meromorphic cocycles*. Preprint.

[Das] S. Dasgupta, *Stark-Heegner points on modular Jacobians*, Ann. Sci. École Norm. Sup. (4) **38** (2005), no.3, 427–469.

[Gr] M. Greenberg. *Heegner point computations via numerical p-adic integration*. Algorithmic number theory, 361–376, Lecture Notes in Comput. Sci., **4076**, Springer, Berlin, 2006.

[GS] R. Greenberg, G. Stevens, *p-adic L-functions and p-adic periods of modular forms*. Invent. Math. **111** (1993), 407–447.

[GvdP] L. Gerritzen and M. van der Put. *Schottky groups and Mumford curves*. Lecture Notes in Mathematics, **817**. Springer, Berlin, 1980.

[Ih] Y. Ihara. *On congruence monodromy problems*. Reproduction of the Lecture Notes: Volume 1 (1968) Volume 2 (1969)(University of Tokyo), with author's notes (2008). MSJ Memoirs, **18**. Mathematical Society of Japan, Tokyo, 2008.

Department of Mathematics, McGill University
Montreal, Canada
E-mail address: darmon@math.mcgill.ca